

# METHOD FOR DATA RECORDING AND READOUT, RECORDING DEVICE, READOUT DEVICE, AND WRITING DEVICE

**Publication number:** JP2000341265

**Publication date:** 2000-12-08

**Inventor:** KATSUTA NOBORU; KAWADA KOJI; HARADA TOSHIHARU; TATEBAYASHI MAKOTO

**Applicant:** MATSUSHITA ELECTRIC IND CO LTD

**Classification:**

- international: **G06F12/14; G06F3/06; G06F21/24; G11B20/10; G11C16/02; H04L9/10; G06F12/14; G06F3/06; G06F21/00; G11B20/10; G11C16/02; H04L9/10; (IPC1-7): H04L9/10; G06F3/06; G06F12/14; G11B20/10; G11C16/02**

- european:

**Application number:** JP19990149892 19990528

**Priority number(s):** JP19990149892 19990528

[Report a data error here](#)

## Abstract of JP2000341265

**PROBLEM TO BE SOLVED:** To make it difficult to make an illegal machine by reproducing contents data while ignoring permission information by recording data, ciphered on the basis of a key or recording data ciphering generated on the basis of recording and readout limitation information and a recording media key provided for recording equipment, and the recording and readout limitation information. **SOLUTION:** Data to be recorded are given a permission code of transmission and reception limitation information for respective categories. The categories may be the equipment number of equipment connected to equipment which records the data. The permission code is given for every category; and 0 indicates permission and 1 indicates nonpermission. The data are ciphered by using as a ciphering key K-CONT calculated from a function (f) depending upon the recording medium key Km of the recording equipment in addition to the permission information P. The function (f) may be a function which employs as an arithmetic result the output obtained by inputting P and Km as a key for block ciphering and a data input.

制限情報							
カテゴリー	1	2	3	...	i	...	Nn
許可符号	p1	p2	p3	...	pi	...	pn

データ	E(M,K_CONT)
-----	-------------

$P = \{p1, p2, p3, \dots, pi, \dots, pn\}$ : コンテンツ送受信先制限情報

$K\_CONT = f(P, K_m)$ : コンテンツ暗号化鍵

$f()$ : コンテンツ暗号化関数

$pi = \begin{cases} 0 & \text{許可} \\ 1 & \text{不許可} \end{cases}$

Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-341265

(P2000-341265A)

(43) 公開日 平成12年12月8日 (2000.12.8)

(51) Int.Cl.<sup>7</sup>

識別記号

FI

テ-マ-ト (参考)

H04L 9/10

G06F 3/06

12/14

G11B 20/10

G11C 16/02

304

320

H04L 9/00

G06F 3/06

12/14

G11B 20/10

G11C 17/00

621Z 5B017

304M 5B026

320B 5B066

H 5D044

601P 5J104

審査請求 未請求 請求項の数10 OL (全13頁)

(21) 出願番号

特願平11-149892

(22) 出願日

平成11年5月28日 (1999.5.28)

(71) 出願人 000003821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 勝田 昇

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 河田 浩嗣

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 10009/445

弁理士 岩橋 文雄 (外2名)

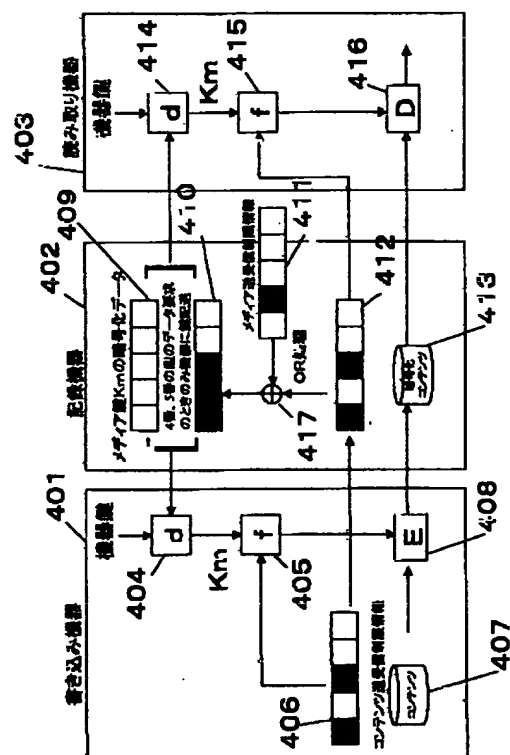
最終頁に続く

(54) 【発明の名称】 データ記録および読み出し方法および記録装置および読み取り装置および書き込み装置

(57) 【要約】

【課題】 本発明は、データの記録および読み出しに際してデータ作成者が許可した機器からだけに記録、読み出しを許すデータ記録方法および読み出し、書き込み方法および装置を提供する。

【解決手段】 データにデータが記録された機器から書き込み読み出しを許す機器についての許可情報をのせ、記録機器では、機器内にある許可情報とデータにある許可情報の両方から判断して読み書きを許す。さらにデータ記録に際しては、記録機器にあるメディア鍵とデータにある許可情報に依存した暗号化鍵でデータを暗号化する。



## 【特許請求の範囲】

【請求項1】データをその記録者が意図したものにのみ読み出し可能にするためのデータ記録機器へのデータ記録方法において

複数の読み出しおよび書き出し対象に対する記録および読み出し制限情報と記録する記録機器に設けられた記録メディア鍵とに基づき記録データ暗号化用鍵を生成し、前記暗号化鍵に基づき記録するデータを暗号化処理したのち、

前記暗号化されたデータと前記記録および読み出し制限情報を記録するデータ記録方法。

【請求項2】さらに記録メディア鍵は、記録機器より暗号化されたものを受信し、前記暗号化された記録メディア鍵を所持する機器鍵で復号処理して記録メディア鍵を生成することを特徴とする請求項1記載のデータ記録方法。

【請求項3】読み出し要求を受けたデータについて、そのデータに記述された送信制限情報と機器で所持する機器鍵で暗号化された記録メディア鍵をデータが記録されている記録機器より読み出し、前記送信制御情報と記録メディア鍵に基づき記録データに施された暗号を復号する復号鍵を生成し、

前記復号鍵に基づき読み出しデータを復号処理することを特徴とするデータ読み出し方法。

【請求項4】データを記録するメモリ部とその制御部からなる記録機器において、制御部は、記録メディア鍵を複数の鍵でそれぞれ暗号化したメディア鍵暗号化データ記憶部と前記記録メディア鍵を暗号化した複数の鍵についてそれぞれ送信許可の有無を示す送受信先制限情報記録部と記録するデータ内にあるデータ送受信先制限情報記憶部を具備し、

データ記録時、記録データにあるデータ送受信先制限情報を保持し、メディア鍵暗号化データについての読み出しリクエスト受信時、前記保持したデータ送受信先制限情報とメディア内送受信先制限情報記憶部にあるメディア内送受信先制限情報に基づき暗号化データ記憶部内のメディア鍵暗号化データ送出を制御し、データ記録時に、前記記録データより読み出し保持した送受信先制限情報を記録データとともに記録することを特徴としたデータ記録装置。

【請求項5】データを記録するメモリ部とその制御部からなる記録機器において、制御部は、記録メディア鍵を複数の鍵でそれぞれ暗号化したメディア鍵暗号化データ記憶部と前記記録メディア鍵を暗号化した複数の鍵についてそれぞれ送信許可の有無を示す送受信先制限情報記録部と記録または記録データあるデータ送受信先制限情報記憶部を具備し、

記録されたデータ出力時、読み出し要求データについてそのデータと送受信先制限情報を記録または読み出し対象データに関する送受信先制限情報として読み出し保持

し、読み出し機器からのメディア鍵暗号化データの要求信号に対し、指示されたメディア鍵暗号化データについて、前記読み出し保持した対象データに関する送受信先制限情報とメディア内送受信先制限情報記憶部にある制限情報に基づき送出制御することを特徴とするデータ記録装置。

【請求項6】メディア内送受信先制限情報は、許可しない機器鍵に対応する鍵暗号化データを所定の許可しないことを意味する固定データとして、記憶されることを特徴とする請求項4記載にデータ記録装置。

【請求項7】メディア内送受信先制限情報は、許可しない機器鍵に対応する鍵暗号化データを所定の許可しないことを意味する固定データとして、記憶されることを特徴とする請求項6記載にデータ記録装置。

【請求項8】書き込みデータを暗号化するデータ暗号化手段と機器に付与された機器鍵を記憶する機器鍵記憶手段を具備し、

データ書き込み時、書き込みデータについての送受信先制限情報を送信し、機器鍵記憶手段に所持している機器鍵によって暗号化された鍵暗号化データを記録機器に要求し、要求にしたがって鍵暗号化が送出されきた場合のとき、前記鍵暗号化データを復号してメディア鍵情報を生成し、前記送信した書き込みデータに関する送受信先制限情報に基づきデータ暗号化鍵を生成し、前記データ暗号化鍵によりデータをデータ暗号化手段で暗号化処理して記録機器に送出することを特徴とするデータ書き込み装置。

【請求項9】読み出しデータを暗号復号化処理する暗号化復号処理手段と機器鍵記憶手段と機器鍵および入力データにより読み出しデータを暗号復号化する暗号復号化鍵を生成制御する制御手段を具備し、

データ読み出し時、制御手段は、その読み出しデータを記録機器に指定し、さらに機器鍵記憶手段内にある機器鍵で暗号化された記録メディア鍵暗号化データ送信を記録機器に要求し、その結果、送信されてきた記録メディア鍵暗号化データを機器鍵に基づき復号処理して記録メディア鍵を生成し、さらに読み出しデータに対応した送受信先制限情報を記録機器より受信し、前記生成した記録メディア鍵と送受信先制限情報に基づきデータ復号鍵を生成することを特徴とするデータ読み出し装置。

【請求項10】データを書き込みおよび読み出し可能な記録機器において、

記録機器に接続機器を限定する送受信先限定情報記憶手段と記録されるデータに付加された書き込み機器または読み出し機器を限定する送受信先限定情報読み取り手段を具備し、

書き込み機器および読み取り機器が接続され、データを書き込みあるいは読み取り処理される際、前記送受信先限定情報記憶手段に記憶された送受信先限定情報と前記送受信先限定情報読み取り手段で読み取ったデータに付

加された送受信先制限情報に基づき、データの記録および送出を制御することを特徴とするデータ記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、音楽データや映画などの映像データなど著作権者が不正なデータの複製を拒否しているデータについて、録画や録音機器で不正に複製されることを防ぐためのデータ記録方法およびその読み出し方法および書き込み方法とその装置に関するものである。

【0002】

【従来の技術】従来の録画機器や録音機器における著作権を保護するものとしては、たとえば、ディジタルオーディオのシリアルインターフェイスにおけるシリアルコピーマネージメントがある。これは、複製の許可情報をチャンネルステータス信号上に載せたものであるが、その情報が容易に改ざん可能であった。それを改善する方法としてたとえば、特願平4-157718号公報にコピーの許可情報記述方法についての記述がある。図11は、従来の記録および伝送時許可情報記述方法の説明図である。同図において、許可コードは、それぞれのカテゴリー毎に設けられており、複製の許可不許可は、各カテゴリー内のコード1およびコード2の存在によって表現される。コード2は、コード1を一方方向性の関数で処理した結果選られる値になっており、コード2からコード1を算出することは困難になっている。

【0003】したがって、特定のカテゴリーについて複製を許可しない場合、コード1を取り除くことで不許可を表現する。そうすることで不許可を示す状態からコード1を生成して許可を示す情報を付加することは困難である。また、コード2に関するすべてのデータよりコンテンツデータを暗号化する暗号化鍵を生成し、コンテンツデータを暗号化しているため、複製許可情報を改ざんするとコンテンツデータを複製するための復号鍵を生成できなくなるため、許可情報を不正に改ざんできなくなることが出来る。

【0004】

【発明が解決しようとする課題】しかしながら、前記従来の許可情報の記述方法では、コンテンツデータを暗号化する暗号化鍵を生成するパラメータが許可情報内に存在するため、暗号化鍵生成方法および暗号化アルゴリズムが秘密であることにのみ不正なコンテンツデータの解読に対する安全性が依存してしまう問題があった。すなわち、特定のカテゴリーにおけるコード1とコード2の関係を無視してもコード2からコンテンツデータ暗号データを復号することは可能であり、特定のカテゴリーの機器が不正な機器を作って自分のカテゴリーで許可されていないものまでも再生し不正することが可能である問題があった。

【0005】以上のような問題点を鑑み本発明は、記録

データだけからでは、許可情報を無視してコンテンツデータを再生し、不正な機器作ることが困難なデータ記録方法および読み出し方法、およびその装置を提供することを目的とする。

【0006】

【課題を解決するための手段】前記課題を解決するために本発明は、データをその記録者が意図したものにのみ読み出し可能にするためのデータ記録機器へのデータ記録方法において複数の読み出しおよび書き出し対象に対する記録および読み出し制限情報と記録する記録機器に設けられた記録メディア鍵とに基づき記録データ暗号化用鍵を生成し、前記暗号化鍵に基づき記録するデータを暗号化処理したのち、前記暗号化されたデータと前記記録および読み出し制限情報を記録するものである。

【0007】また、本発明は、読み出し要求を受けたデータについて、そのデータに記述された送信制限情報と機器で所持する機器鍵で暗号化された記録メディア鍵をデータが記録されている記録機器より読み出し、前記送信制限情報と記録メディア鍵に基づき記録データに施された暗号を復号する復号鍵を生成し、前記復号鍵に基づき読み出しデータを復号処理するものである。

【0008】また、本発明は、データを記録するメモリ部とその制御部からなる記録機器において、制御部は、記録メディア鍵を複数の鍵でそれぞれ暗号化したメディア鍵暗号化データ記憶部と前記記録メディア鍵を暗号化した複数の鍵についてそれぞれ送信許可の有無を示す送受信先制限情報記録部と記録するデータ内にあるデータ送受信先制限情報記憶部を具備し、データ記録時、記録データにあるデータ送受信先制限情報を保持し、メディア鍵暗号化データについての読み出しリクエスト受信時、前記保持したデータ送受信先制限情報とメディア内送受信先制限情報記憶部にあるメディア内送受信先制限情報に基づき暗号化データ記憶部内のメディア鍵暗号化データ送出を制御し、データ記録時に、前記記録データより読み出し保持した送受信先制限情報を記録データとともに記録するデータ記録装置の構成である。

【0009】また、本発明は、データを記録するメモリ部とその制御部からなる記録機器において、制御部は、記録メディア鍵を複数の鍵でそれぞれ暗号化したメディア鍵暗号化データ記憶部と前記記録メディア鍵を暗号化した複数の鍵についてそれぞれ送信許可の有無を示す送受信先制限情報記録部と記録または記録データあるデータ送受信先制限情報記憶部を具備し、記録されたデータ出力時、読み出し要求データについてそのデータと送受信先制限情報を記録または読み出し対象データに関する送受信先制限情報として読み出し保持し、読み出し機器からのメディア鍵暗号化データの要求信号に対し、指示されたメディア鍵暗号化データについて、前記読み出し保持した対象データに関する送受信先制限情報とメディア内送受信先制限情報記憶部にある制限情報に基づき送

出制御するデータ記録装置の構成である。

【0010】本発明は、メディア内送受信先制限情報は、許可しない機器鍵に対応する鍵暗号化データを所定の許可しないことを意味する固定データとして、記憶されるデータ記録装置の構成である。

【0011】また、本発明は、メディア内送受信先制限情報は、許可しない機器鍵に対応する鍵暗号化データを所定の許可しないことを意味する固定データとして、記憶されるデータ記録装置の構成である。

【0012】また、本発明は、書き込みデータを暗号化するデータ暗号化手段と機器に付与された機器鍵を記憶する機器鍵記憶手段を具備し、データ書き込み時、書き込みデータについての送受信先制限情報を送信し、機器鍵記憶手段に所持している機器鍵によって暗号化された鍵暗号化データを記録機器に要求し、要求にしたがって鍵暗号化が送出されきた場合のとき、前記鍵暗号化データを復号してメディア鍵情報を生成し、前記送信した書き込みデータに関する送受信先制限情報に基づきデータ暗号化鍵を生成し、前記データ暗号化鍵によりデータをデータ暗号化手段で暗号化処理して記録機器に送出するデータ書き込み装置の構成である。

【0013】また、本発明は、読み出しデータを暗号復号化処理する暗号復号化処理手段と機器鍵記憶手段と機器鍵および入力データにより読み出しデータを暗号復号化する暗号復号化鍵を生成制御する制御手段を具備し、データ読み出し時、制御手段は、その読み出しデータを記録機器に指定し、さらに機器鍵記憶手段内にある機器鍵で暗号化された記録メディア鍵暗号化データ送信を記録機器に要求し、その結果、送信されてきた記録メディア鍵暗号化データを機器鍵に基づき復号処理して記録メディア鍵を生成し、さらに読み出しデータに対応した送受信先制限情報を記録機器より受信し、前記生成した記録メディア鍵と送受信先制限情報に基づきデータ復号鍵を生成することを特徴とするデータ読み出し装置の構成である。

【0014】また、本発明は、データを書き込みおよび読み出し可能な記録機器において、記録機器に接続機器を限定する送受信先限定情報記憶手段と記録されるデータに付加された書き込み機器または読み出し機器を限定する送受信先限定情報読み取り手段を具備し、書き込み機器および読み取り機器が接続され、データを書き込みあるいは読み取り処理される際、前記送受信先限定情報記憶手段に記憶された送受信先限定情報と前記送受信先限定情報読み取り手段で読み取ったデータに付加された送受信先限定情報に基づき、データの記録および送出を制御するデータ記録装置の構成である。

【0015】

【発明の実施の形態】以下、本発明の実施の形態について図1から図10を用いて説明する。

【0016】図1は、本実施の形態における記録データ

の記録時におけるデータ構成の説明図である。同図において、記録されるデータには、各カテゴリーに対する送受信の制限情報の許可符号が付与される。このカテゴリーは、このデータが記録されている機器に接続される機器の機器番号でもよいし、機器に与えられている鍵の番号などである。許可符号は、各カテゴリー毎に与えられ、それぞれ0が許可、1が不許可を示す。データは、この許可情報Pに加えて記録されている記録機器にある記録メディア鍵 $K_m$ に依存した関数 $f$ により算出された $K\_CONT$ を暗号化鍵として暗号化する。関数 $f$ は、たとえば、ブロック暗号の鍵およびデータ入力にPおよび $K_m$ を入力してその出力を演算結果とするものでよい。

【0017】以上のように構成されたデータにおいては、各カテゴリーに示された許可コードは、データを暗号化する暗号化鍵を生成するパラメータになっているため、改ざんするとデータを復号するための鍵が作れなくなるため改ざんできない。また、記録メディア鍵 $K_m$ がデータ上に存在しないため、図1に示すデータを伝送路で盗聴あるいは記録機器からコピーされても暗号化されたデータを復号するための鍵を得ることができないため、データを再生できず不正な複製の作成を困難にできる。したがって、許可情報Pにしたがって許された機器へ記録メディア鍵 $K_m$ を伝送し、図1に示されるデータを送信記録するすべての記録、読み出し方法およびそれを実現する機器に本発明が適応できる。

【0018】図2は、本発明の実施の形態における記録機器およびそれにデータを書き込む書き込み機器の構成図である。同図において1は、データ書き込み機器、2は、データ記録機器、3は、書き込み機器1に与える機器鍵を記憶する機器鍵記憶部、4は、書き込み機器1と記録機器2での伝送路におけるデータの入出力制御を行う入出力制御部、5は、コンテンツデータを暗号化処理する暗号化処理部、6は、記録機器へ記録するデータを書き込み機器側で記録しているコンテンツ記録部、7は、図1の示した各カテゴリーの機器に与えられる機器鍵に基づきそれぞれ暗号化されてメディア鍵を記憶する鍵暗号化データ記憶部、8は、記憶機器内にあらかじめ与えられた各カテゴリーへの送受信の制限情報を記憶するメディア内送受信先制限情報記憶部、9は、送信されてくるコンテンツの送受信先制限情報を一時保持するコンテンツ送受信先制限情報記憶部、10は、書き込み機器との入出力制御部、11は、データ記録部である。

【0019】以上の構成において、以下その動作を説明する。まず、書き込み機器1は、PCなどのような内部で生成あるいはネットワーク等を介して取り込んでコンテンツデータをハードディスクなどの記録部に蓄えたものをメモリーカードなどの記録機器へ記録するような場合が考えられる。したがって、書き込み機器と記録機器間の基本的なデータの送受信は、たとえば、現在の

PCとメモリカード間で行われている方法など一般に公知な方法を用いて行えるため、機器間を流れる情報について詳細に説明する。図2において、書き込み機器1と記録機器2間のデータ送受信は、入力制御部4および入力制御部10で行われる。

【0020】図6は、入力制御部4および10で行われる処理フローを示した説明図である。同図において201は、書き込みリクエストおよびコンテンツ送受信先制限情報送出处理、202は、鍵暗号化データリクエスト番号送出处理、203は、記録メディア鍵復号処理、204は、コンテンツ暗号化鍵生成処理、205は、コンテンツ暗号化送出处理、206は、コンテンツ送受信先制限情報読み取り処理、207は、リクエスト番号有効性確認処理、208は、メディア鍵暗号化データ送出处理、209は、コンテンツデータ記録処理である。同図で左側に示された処理が図2における入出力制御処理4の処理であり、右側が入出力制御処理10の処理である。まず、入出力制御部4は、記録機器2へ記録するため、書き込みリクエスト信号とともにコンテンツ記録部6より送信するコンテンツに対するコンテンツ送信先制限情報Pを読み出し、入出力制御部10へ送信する。入出力制御部10は、コンテンツ送受信先制限情報記憶部9へ記録する。次に、入力制御部4は、メディア鍵暗号化データリクエスト番号送出处理202において、機器鍵記録部3に記録された鍵が対応しているカテゴリ番号をリクエスト番号として入出力制御部10へ送出する。次にリクエスト有効性確認処理207でコンテンツ送受信先制限情報記憶部9とメディア内送受信先制限情報記憶部8内のデータに基づき各カテゴリに対する許可内容を確認する。図5は、メディア内送受信先制限情報P dの説明図である。図1におけるPと同様に各カテゴリに対して記録機器製造時に送受信を禁じたカテゴリについて不許可の符号を与えたものである。図8は、コンテンツ送信先制限情報とメディア送受信先制限情報から送受信先の制限情報P dを算出する処理の説明図である。P c dの各カテゴリに対する要素は、PおよびP dの各要素のOR処理によって生成される。そして、このように算出されたP c dに基づいてリクエスト番号に対応するカテゴリの許可符号が0であれば、許可あり判定し、メディア鍵暗号化データ送出处理208進み、そうでないときは、許可が否決されたとして処理を終了する。図9は、カテゴリ数が6の場合での具体的な送受信先制限情報P c dの算出例の説明図である。コンテンツ側でカテゴリ1と4と6について不許可であり、メディア側でカテゴリ4と5について不許可であるとき、送受信先制限情報は、カテゴリ2と3のみ0となり許可をしめすことになる。

【0021】図6のフローに戻って、メディア鍵暗号化データ送出处理208では、リクエスト番号に対応するカテゴリに番号のメディア鍵暗号化データをメディア

鍵暗号化データ記憶部7より選択して送出する。図4は、メディア鍵暗号化データの説明図である。各カテゴリに対するデータは、記録メディア鍵K mをそれぞれのカテゴリiに付与された機器鍵S iで暗号化されたデータになっている。したがって、リクエストされたカテゴリ番号の鍵を用いれば、復号処理によりK mが生成できるデータが選択され送出される。

【0022】記録メディア鍵復号処理203では、送られてきたメディア鍵暗号化データを機器鍵記憶部3にあるデータに基づき復号処理してK mを得る。次に、コンテンツ暗号化鍵生成処理204では、K mとPよりf (P K m)を演算処理してコンテンツ暗号化鍵K \_CONTを生成する。そしてコンテンツ暗号化送出处理205では、コンテンツ記録部6より書き込むデータを暗号化処理部5に送り、コンテンツ暗号化鍵K \_CONTにより暗号化したデータを入出力処理部4を介して入出力処理部10へ送出する。入出力処理部10では、コンテンツデータ記録処理209で、送信されてきたデータにコンテンツ送受信先制限情報記憶部9に記録されたデータをコンテンツ送受信制限情報を付加して図1に示したデータとして記録する。

【0023】以上のような動作により、書き込み機器および記録機器間では、図1で示したデータと書き込み機器鍵で暗号化された記録メディア鍵K mであるため、許可されたカテゴリの機器以外にとっては、たとえば、通信路を盗聴したとしてもコンテンツを再生することが困難であり不正な複製を生成することができないようにできる。

【0024】また、記録機器内にも送受信先制限情報を設けることにより、コンテンツおよび記録機器に入れられたどちらか最新の許可情報を有効にすることができ、より高い著作権保護能力が実現できる。すなわち、非常に以前に送信されたデータにつけられた送受信先制限情報では、数年たって、その後に作られた不正な機器については、それを不許可にすることが困難であるが、記録機器側により新しい制限情報があれば、コンテンツの流通後に発覚した不正機器についても排除が可能になる。また、逆に古い記録機器には、制限状態がほとんどないが、新しいコンテンツを記録された制限情報に基づいてコンテンツ側で排除したいカテゴリを指定することでより高い著作権保護が実現できる。

【0025】図3は、記録機器からの読み出しを行う読み出し機器と記録機器の構成を示した構成図である。同図において、101は、読み出し機器、102は、記録機器、103は、機器鍵記憶部、104は、入出力制御部、105は、コンテンツに施された暗号を復号する復号化部、106は、コンテンツ送受信先制限情報記憶部、107は、復号されたコンテンツデータを再生する再生処理部、108は、鍵暗号化データ記憶部、109は、メディア内送受信先制限情報記憶部、110は、入



出力制御部、111は、コンテンツ送受信先制限情報記憶部、112は、記録部である。

【0026】以上のような構成において以下その動作を説明する。読み出し機器101内の機器鍵記憶部103は、図2における機器鍵記憶部3と同様機器に与えられた機器鍵を記憶する。

【0027】記録機器102内のメディア鍵暗号化データ記憶部107およびメディア内送受信先制限情報記憶部108およびコンテンツ送受信先情報記憶部109は、図2の記録機器2におけるメディア鍵暗号化データ記憶部7およびメディア内送受信先制限情報記憶部8およびコンテンツ送受信先情報記憶部9と同等の機能を持ち出力制御部110により制御される。読み出し機器および記録機器間の送受信は、入出力制御部104および入出力制御部110で制御され行われる。

【0028】図7は、読み出し機器および記憶機器間の処理のフローを説明した図である。同図において、301は、読み出しリクエスト送出処理、302は、鍵暗号化データリクエスト番号送出処理、303は、記録メディア鍵復号処理、304は、コンテンツ復号化鍵生成処理、305は、コンテンツ復号および再生処理、306は、コンテンツ送受信先制限情報読み取り処理、307は、リクエスト番号有効性確認処理、308は、メディア鍵暗号化データおよびコンテンツ送受信先制限情報送出処理、309は、コンテンツデータ送出処理である。図7の左側の処理は、入出力制御部104、右側の処理が入出力制御部110の処理のフローである。まず、最初に、入力制御部104は、読み出しリクエスト信号送出処理301により、読み出したいデータを指定する。入力制御部110では、指定されたファイルのコンテンツ送受信先制限情報を読み取りコンテンツ送受信先制限情報記憶部111に記憶保持する。次に、入出力制御部104は、鍵暗号化データリクエスト番号送出処理302において、機器が保持する鍵のカテゴリ番号に相当する番号を入出力制御部110に送る。入出力制御部110は、リクエスト番号有効性確認処理307において、図6におけるリクエスト番号有効性確認処理207と同様にコンテンツ送受信先制限情報およびメディア送受信先制限情報から図8で説明した処理により送受信先制限情報Pcdを生成し、リクエスト番号がPcdで許可されているかを確認判定し、否決の場合は、処理を停止し、許可されている場合は、メディア鍵暗号化データ送出処理308へ進む。メディア鍵暗号化データおよびコンテンツ送受信先制限情報送出処理308では、リクエスト番号に対応する鍵番号に対応する暗号化データを鍵暗号化データ記憶部108より読み出し、入出力制御部104へコンテンツ送受信先制限情報とともに送る。入出力制御部104では、メディア鍵復号処理303において送られた暗号化データを機器鍵記憶部103の記憶する鍵で復号処理してメディア鍵Kmを生成すると

もに、コンテンツ送受信先制限情報コンテンツ送受信先制限情報記憶部106に記憶させる。続いて、コンテンツ鍵復号処理304において、メディア鍵Kmとコンテンツ送受信先制限情報記憶部106内のコンテンツ送受信先制限情報に基づきコンテンツ復号鍵K\_CONTを生成し復号化処理部105にセットし、送信リクエスト信号を入出力制御部110へ送信する。入出力制御部110は、コンテンツデータ送信処理309で送信リクエストに応じてコンテンツデータを入出力制御部104に送信する。入力制御部104は、送信されてきたデータを復号処理部105に送り、暗号復号処理された後、再生部107で再生処理される。

【0029】以上の処理により、データ読み取り機器301は、コンテンツおよび記録機器306にある送受信先制限情報により許可されているカテゴリの機器鍵を持つ時のみデータを読み出すことができ、その他の許可のない機器がデータを読み出すことが困難にすることができる。特に記録機器内と記録されているデータにある両方の受信先制限情報に基づき行えるため、古い著作物で作成当時拒絶の対象とならなかったカテゴリ機器で不正が合った場合にその機器を記録機器にある送受信先制限情報に基づき読み出し困難にすることが出来る。

【0030】図10は、図1のような記述に基づき記録機器に記録し、図2、図3で説明したような読み取り機器、書き込み機器による記録機器への書き込みから読み出しまでの処理を説明した図である。同図において401は書き込み機器、402は、記録機器、403は、読み取り機器、404は暗号解読処理、405は、演算処理、406は、コンテンツ送受信制限情報、407は、コンテンツデータ、408は暗号化処理、409はmメディア鍵暗号化データ、410は、送受信先制限情報、411は、メディア送受信制限情報、412は、コンテンツ送受信制限情報、413は、暗号化コンテンツデータ、414は、暗号復号化処理、415は、演算処理、416は、暗号復号化処理、417は、要素間のOR処理である。

【0031】コンテンツ407を記録機器に記録する場合、コンテンツ送受信先制限情報406を記録機器402に送信する。コンテンツ送受信先制限情報412は、メディア送受信制限情報411とOR処理417で処理され、送受信先制限処理410に変換される。ここで、四角の箱が白である場所が許可されているカテゴリとすると、コンテンツ側から1番目のと3番目が拒否され、記録機器から2番目が拒否され、結果4番目、5番目のカテゴリのみが許可される。書き込み機器が、このカテゴリの機器鍵を持っていたとすると、そのカテゴリ鍵に対応するメディア鍵暗号化データが書き込み機器401に送られ、暗号復号処理404にてメディア鍵Kmが複製される。そのKmとコンテンツ送受信先制限情報406に基づき演算処理405でコンテンツ暗号用の鍵

が生成され、コンテンツを暗号化処理408で暗号化して記録メディアに送られ暗号コンテンツ413に送られ記録される。それを読み取り機器403が読み出す場合、記録機器402は、書き込み時の処理同じ手順で送受信先制限情報410に基づき読み取り機器側の機器鍵のカテゴリーが許可されているかを判定し、許可されている場合は、メディア鍵Kmの暗号化データを送る。

【0032】この場合、同じKmを暗号化しているため、書き込み機器内の機器鍵カテゴリーと読み取り機器内の機器鍵カテゴリーが異なってもかまわない。許可される場合、そのカテゴリーに相当するものを送れば、読み取り機器側でKmを再生できる。そして、コンテンツ送受信制限情報412が読み取り機器に送られ、Kmとともに演算処理fにより演算されてコンテンツ復号用の鍵が書き込み機器で暗号化したものと同じ値で生成される。したがって、暗号化コンテンツ413は、読み取り機器側で再生処理416により、正しく再生できる。

【0033】以上のように、書き込み機器から読み取り機器へ記録機器を介してデータを送ることができ、その間の著作権情報である送受信先制限情報は、改ざんされない様に守れかつその情報が示す許可された機器に対して盗聴が困難な状態で送受信することが出来る。

【0034】なお、本実施の形態では、送受信先制限情報は許可不許可の表現を各カテゴリーに対して許可を0、不許可を1としたビット列で表現したが、それをランレングスコーディングしたものでもよいし、もっと別な変換処理した形式で表現してもよい。また、送信先制御情報を伝送する際、特に暗号化せずに送ったが、書き込み時に制限情報により不許可にならない様に送受信先制限情報を改ざんし、読み取り時に全く同じ改ざんを行われることで制限情報を回避させない様に、送信時、暗号化したり、チェックサムをつけて改ざんを検出可能にすることが出来る。

【0035】また、暗号コンテンツの暗号部以外においても暗号処理を行っているのを図2、図3では入出力制御部で行っているが、これらは、通常暗号化データ数も少なく高速処理も要求されないものでソフトウェア的に十分可能であり、制御部内での処理として説明したが、それらの機器をハード的に構成することも可能である。また、図2、図3で示した構成以外でも同様の処理が可能で構成であればよい。

【0036】また、メディア送信先制限情報とコンテンツ側の送信先制限情報をそれぞれ記憶部を設けて要素毎のOR処理を施して最終的な制限情報を導き出したが、結果的にそれと同様のカテゴリーが不許可となるように判定できれば、他の方法でもよい。たとえば記録メディア送受信先制限情報は、鍵暗号化データ中から不許可部分のデータを抜き取ることで表現することもでき、それからコンテンツ送受信制御情報を使って同様の判定結果を得てもよい。

【0037】また、本実施の形態では、送受信先制限情報からデータの暗号化鍵を生成させることで改ざんを防いでいるがデータに関連づける別の方法を用いても同様の効果選られる。たとえば、コンテンツデータを暗号化する暗号化鍵が別ファイルとして存在する場合は、そのファイル内のデータとしていっしょに記録するとともにファイル全体を改ざん防止のためのチェックサム等を用いることでコンテンツデータとの関連づけが可能となる。

【0038】また、本実施の形態では、各カテゴリーの許可情報は、記録データの送受信先への許可情報としたが、それ以外の情報を意味するデータとして利用も可能である。たとえば、コピー禁止情報等のフラグとしても利用可能である。

【0039】また、本実施の形態では、書き込み時についても制限情報を適応したが、読み込み時のみにこれを適応しただけでも書き込まれたデータを読み出すときに不正な機器での再生を困難にする効果を実現できる。

【0040】また、本実施の形態で示した書き込み、読み出し手順以外でもコンテンツにある制限情報と記憶機器側にある制限情報に基づき送受信を制限するのであれば、その手続きなどの順番がことなってもよいし、異なる処理が挿入されてもよい。

【0041】また、本実施の形態では、書き込み機器は、機器内の記録部にあるデータを記録機器に書き込んだが、書き込み機器に入力されてくるデータを記録機器に書き込む際にも同様に本発明を用いることが可能である。

【0042】

【発明の効果】以上説明したように、本発明によれば、データを記録機器に書き込み読み出しする際に、記録機器内にある送受信先限定情報とデータに付加された送受信先限定情報によりデータの書き込み読み出しを制御するので双方の制限情報のうちより新しい情報に基づき不正機器を排除することができる。また、データに、付加する許可情報をデータの暗号化鍵の生成パラメータとして用いることで改ざんを防止するとともに、暗号化鍵生成パラメータとして記録機器にある鍵パラメータを用いることによりデータを復号するために必要なパラメータを記録データとは別に存在させることができ、単に通信路を盗聴しただけでは解読するための情報を入手できない様にすることができ、より不正が行うことが困難な著作権保護を実現できるデータ記録方法、読み出し方法および記録機器、読み出し機器、書き込み機器を提供することができ、本発明の実用的効果は大きい。

【図面の簡単な説明】

【図1】本実施の形態における記録データの記録時におけるデータ構成の説明図

【図2】本発明の実施の形態における記録機器およびそれにデータを書き込む書き込み機器の構成図



【図3】本発明の実施の形態における記録機器からの読み出しを行う読み出し機器と記録機器の構成図

【図4】本発明の実施の形態におけるメディア鍵暗号化データの説明図

【図5】本発明の実施の形態におけるメディア内送受信先制限情報Pdの説明図

【図6】本発明の実施の形態における入力制御部4および10で行われる処理フローを示した説明図

【図7】本発明の実施の形態における読み出し機器および記憶機器間の処理のフローの説明図

【図8】本発明の実施の形態におけるコンテンツ送信先制限情報とメディア送受信先制限情報から送受信先の制限情報Pdを算出する処理の説明図

【図9】本発明の実施の形態における送受信先制限情報Pcdの算出例の説明図

【図10】本発明の実施の形態における読み取り機器、書き込み機器による記録機器への書き込みから読み出しまでの処理の説明図

【図11】従来の記録および伝送時許可情報記述方法の説明図

【符号の説明】

- 1 データ書き込み機器
- 2 データ記録機器
- 3 機器鍵記憶部
- 4 入出力制御部
- 5 暗号化処理部
- 6 コンテンツ記録部
- 7 鍵暗号化データ記憶部
- 8 メディア内送受信先制限情報記憶部
- 9 コンテンツ送受信先制限情報記憶部
- 10 書き込み機器との入出力制御部
- 11 データ記録部
- 101 読み出し機器

- 102 記録機器
- 103 機器鍵記憶部
- 104 入出力制御部
- 105 コンテンツに施された暗号を復号する復号化部
- 106 コンテンツ送受信先制限情報記憶部
- 107 復号されたコンテンツデータを再生する再生処理部
- 108 鍵暗号化データ記憶部
- 109 メディア内送受信先制限情報記憶部
- 110 入出力制御部
- 111 コンテンツ送受信先制限情報記憶部
- 112 記録部
- 201 書き込みリクエストおよびコンテンツ送受信先制限情報送出処理
- 202 鍵暗号化データリクエスト番号送出処理
- 203 記録メディア鍵復号処理
- 204 コンテンツ暗号化鍵生成処理
- 205 コンテンツ暗号化送出処理
- 206 コンテンツ送受信先制限情報読み取り処理
- 207 リクエスト番号有効性確認処理
- 208 メディア鍵暗号化データ送出処理
- 209 コンテンツデータ記録処理
- 301 読み出しリクエスト送出処理
- 302 鍵暗号化データリクエスト番号送出処理
- 303 記録メディア鍵復号処理
- 304 コンテンツ復号化鍵生成処理
- 305 コンテンツ復号および再生処理
- 306 コンテンツ送受信先制限情報読み取り処理
- 307 リクエスト番号有効性確認処理
- 308 メディア鍵暗号化データおよびコンテンツ送受信先制限情報送出処理
- 309 コンテンツデータ送出処理

【図4】

【図5】

鍵暗号化データ

{Ed(Km,S1),Ed(Km,S2),Ed(Km,S3),...,Ed(Km,Sl),...,Ed(Km,Sm)}

Ed():暗号化アルゴリズム

メディア内送受信先制限情報

Pd={pd1,pd2,pd3,...,pdi,...,pdcn}

$Pdi = \begin{cases} 0 & \text{許可} \\ 1 & \text{不許可} \end{cases}$

【図9】

P={1, 0, 0, 1, 0, 1}:コンテンツ送受信先制限情報

Pd={0, 0, 0, 1, 1, 0}:メディア送受信先制限情報



送受信先制限情報

Pcd={1, 0, 0, 1, 1, 1}

【図1】

制限情報					
カテゴリー	1	2	3	...	i ... Nn
許可符号	p1	p2	p3	...	pi ... pn
データ E(M,K_CONT)					

$P=\{p1, p2, p3, \dots, pi, \dots, pn\}$ :コンテンツ送受信先制限情報

$K\_CONT = f(P, K\_m)$ :コンテンツ暗号化鍵

$f()$ :コンテンツ鍵生成関数

$pi = \begin{cases} 0 & \text{許可} \\ 1 & \text{不許可} \end{cases}$

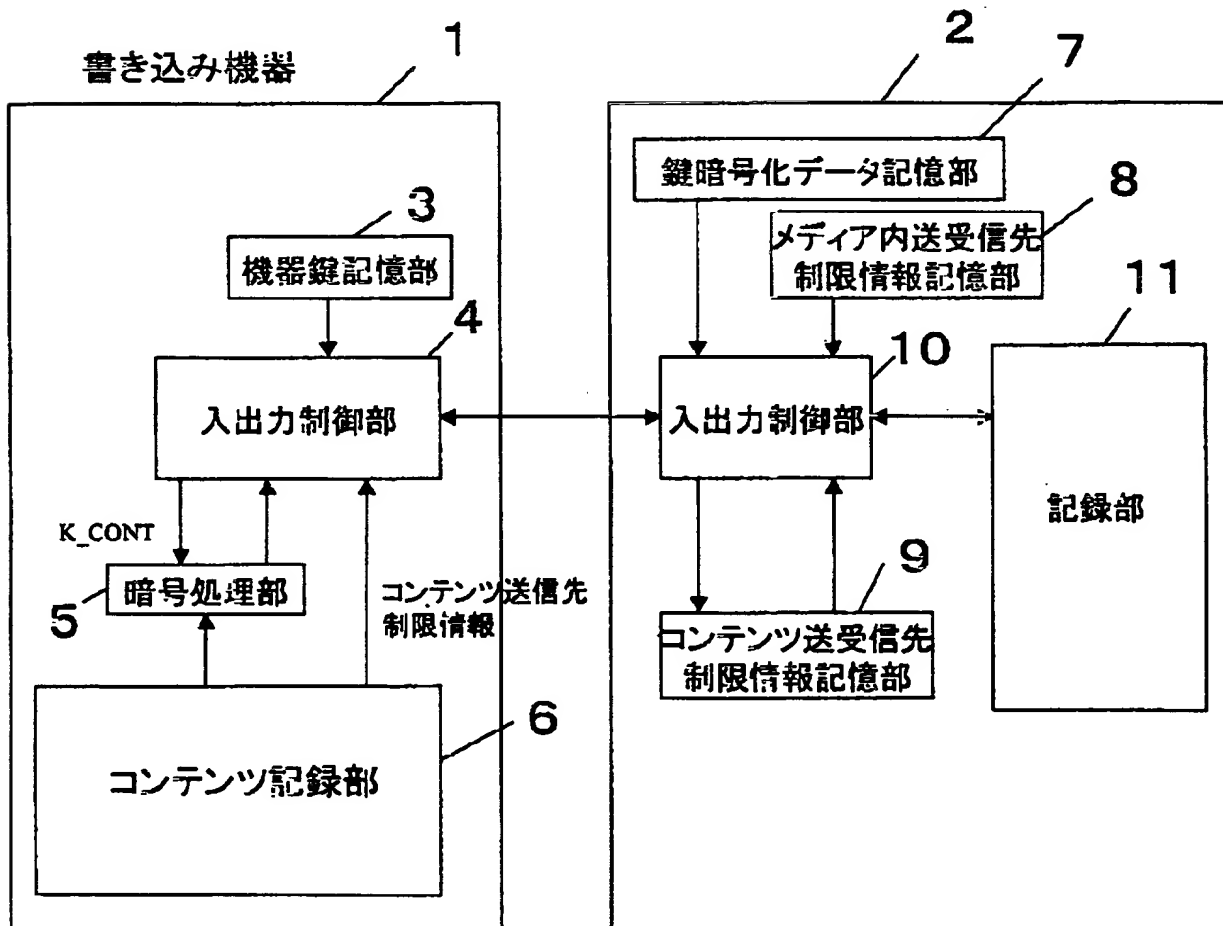
【図11】

	カテゴリー1	カテゴリー2	...	カテゴリーi	...	カテゴリーm
コード1	k1	k2		ki		km
コード2	f(k1)	f(k2)		f(ki)		f(km)
コンテンツデータE(M,F)						

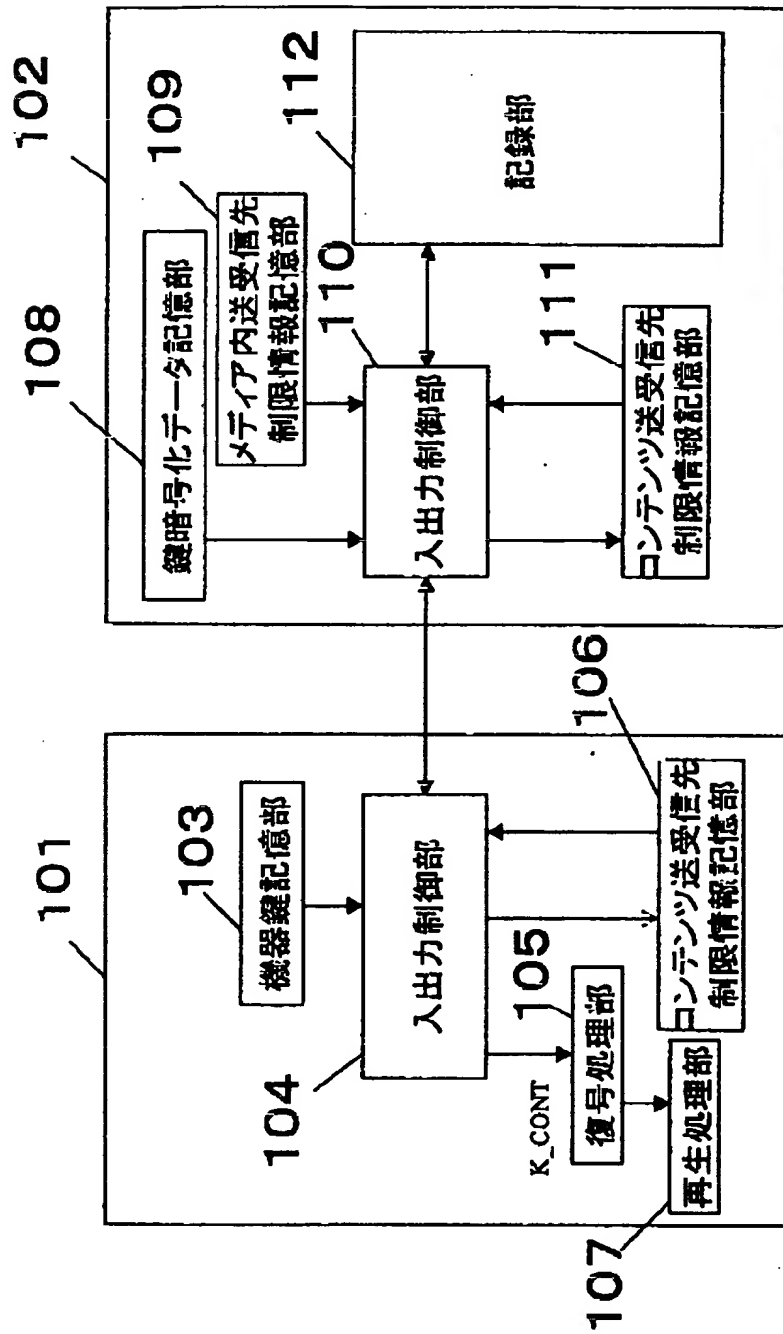
$F:f(k1), f(k2), \dots, f(ki), \dots, f(km)$ より計算される暗号化鍵

$E()$ :暗号処理

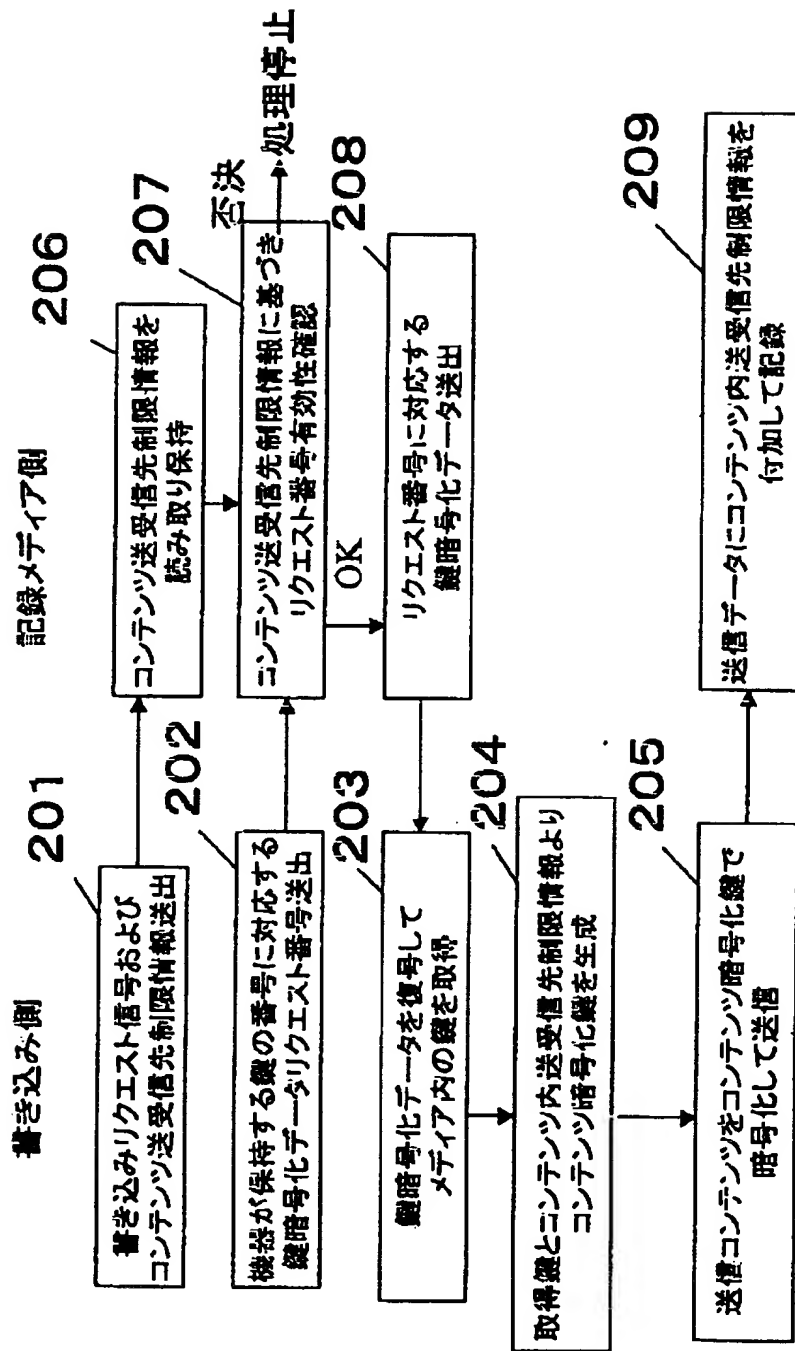
【図2】



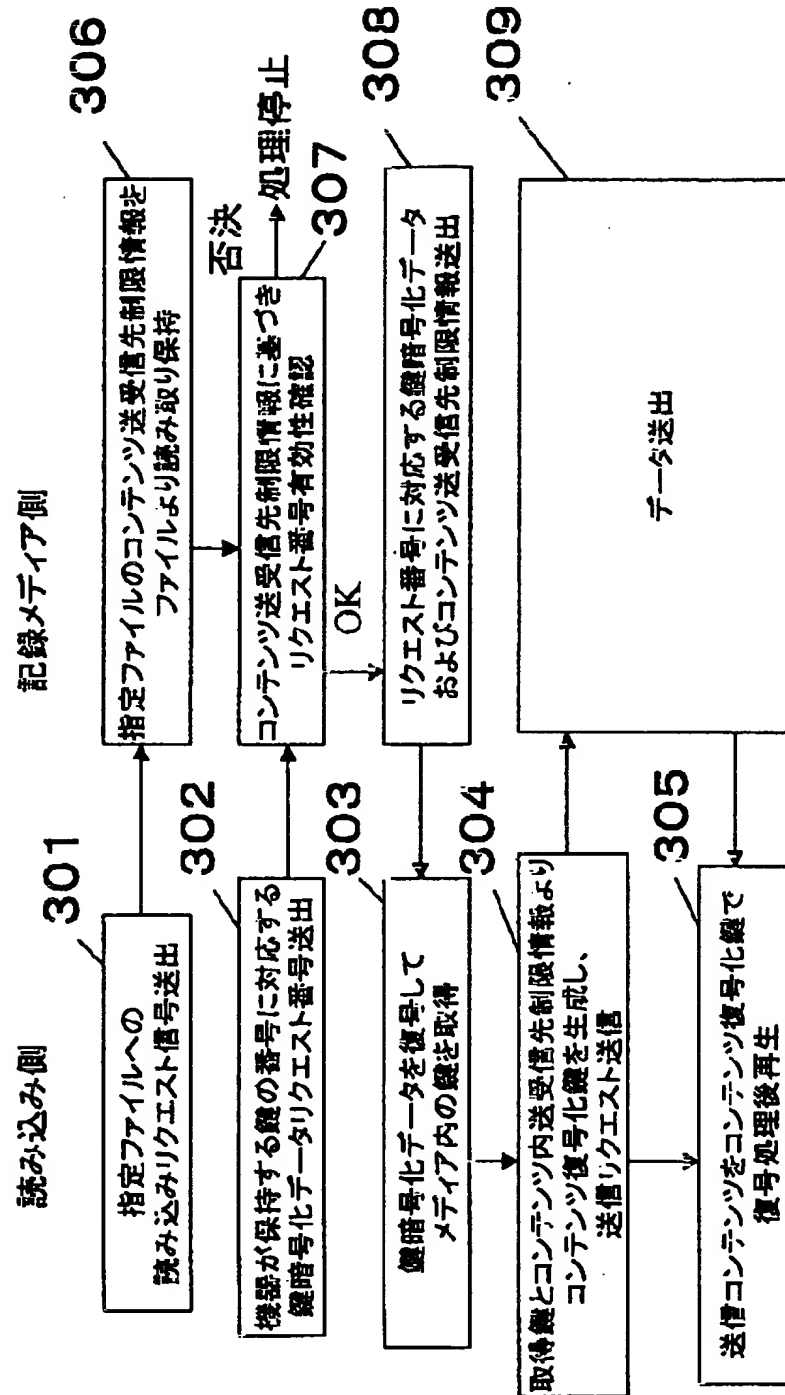
【図3】



【図6】



【図7】



【図8】

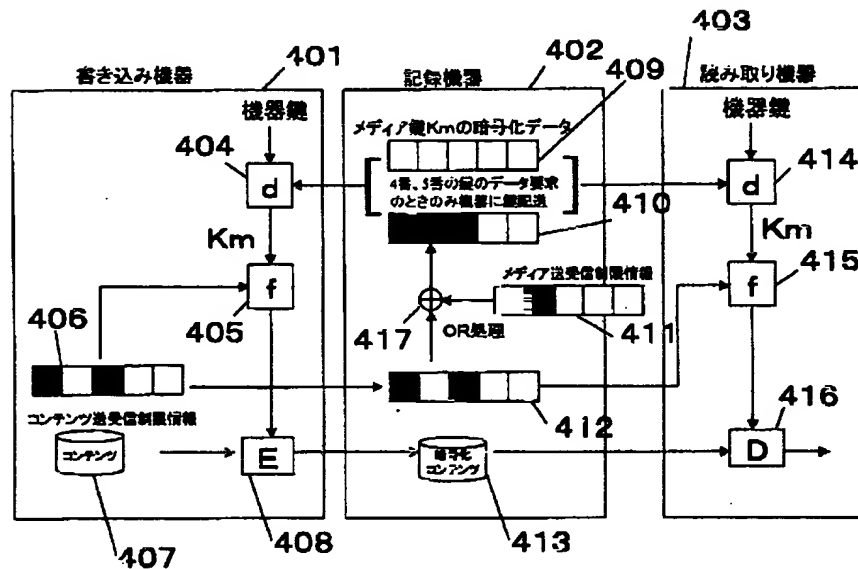
 $P = \{p_1, p_2, p_3, \dots, p_i, \dots, p_n\}$  : コンテンツ送受信先制限情報

 $Pd = \{pd_1, pd_2, pd_3, \dots, pd_i, \dots, pd_n\}$  : メディア送受信先制限情報


送受信先制限情報

 $Pcd = \{pd_1 \wedge p_1, pd_2 \wedge p_2, pd_3 \wedge p_3, \dots, pd_i \wedge p_i, \dots, pd_n \wedge p_n\}$ 
 $\wedge$  : OR処理

【図10】



フロントページの続き

(72)発明者 原田 俊治  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72)発明者 館林 誠  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

F ターム(参考) 5B017 AA06 BA04 BA05 BA07 BB02  
BB03 CA07 CA14 CA16  
5B025 AD14 AE10  
5B065 PA04 PA16  
5D044 DE17 DE50 EF05 FG18 GK12  
GK17  
5J104 AA07 AA13 AA16 AA41 EA18  
GA05 KA02 NA03 NA27 PA14